学校编码：10384　　分类号_____密级_____
学号：X200343029　　UDC _____

厦门大学

硕 士 学 位 论 文

基于 LDAP 统一身份认证的学生信息管理系统的研究与实现

Research and Implement on Students' Information Management System With Uniform Identity Authentication Based on LDAP

陈 志 乾

指导教师姓名：郑 建 德 教授

专 业 名 称 ： 计算机应用技术

论文提交日期：2007 年 5 月

论文答辩时间：2007 年 5 月

学位授予日期：2007 年 月

答辩委员会主席：_____

评 阅 人：_____

2007 年 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：陈志乾

2007 年 5 月 19 日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1、保密（　），在　　年解密后适用本授权书。

2、不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　月　日

导师签名：　　日期：　　年　月　日

摘　要

随着网络技术的发展与应用，随着数字校园网建设的不断完善，网络应用日益丰富，应用服务的增加使得网络管理特别是基于用户和应用的网络管理变得越来越复杂。用户在不同应用中有着不同的权限，每个应用都需要设置帐号，这就带来了许多问题，管理起来很不方便；尤其是用户面对多个应用系统需要输入不同的帐号和口令，不仅烦琐，而且容易出现口令丢失等安全隐患。另外，用户身份认证和安全问题也日益突出。如何使用户只拥有一个单一的帐号，却可以在多个不同的应用系统中加以应用，就成了急待解决的问题。这样不仅能实现多个系统之间的用户身份认证的统一管理，又很大程度上方便了每个用户的操作，提高了网络管理的能力。

针对上述问题,本文首先论述了几种常用的身份认证机制,然后分析了目录服务的优势和应用前景,接着重点研究了 LDAP 协议的四种模型,并就目录信息树进行深入的研究，在充分了解掌握了 LDIF 文件格式和实现原理的基础上，首次自主研发了 LDIF 自动生成系统；然后在系统设计中，对系统的目录树的设计和优化做了一些必要的研究和设计;最后结合校园网的实际应用,考虑到 LDAP 的良好 C/S 特性以及异构网络的优势，研究并实现了基于 LDAP 统一身份认证的学生信息管理系统。

基于 LDAP 统一身份认证的系统主要包括三方面的工作：一是 LDAP 服务器的架设以及用户账户信息的存储；二是应用程序服务器的设计以及和 LDAP 服务器之间的连接；三是客户端的实现，如何连接访问应用程序服务器，并通过应用程序服务器访问 LDAP 服务器，并完成服务器与客户端之间的数据通信。

关键词：LDAP；统一身份认证；管理系统

Abstarct

Along with the network technology development and the application, Along with the unceasing consummation which constructs the digital campus network, the network application are day by day abundance, the unceasing application service causes the network management become more and more complex specially based on the user and the application network management. The user has the different jurisdiction in the different application system, each application system needs to establish the user's account, this has brought many questions, the management of all accounts is not very convenient; The user needs to input the different name and password in particular facing many application systems, not only troublesome, but also easy to appear security hidden troubles and so on password loss. Moreover, the user identity authentication and the security problem day by day are also prominent.How enable the user only to have a sole account number, may perform actually in many different application system to apply, has become the pending issue. Not only it can be realisable to carry out the uniform identity authentication management between different application system, but also has to a great extent facilitated each user's operation, enhanced network management ability.

the article aims at above question,discuss some common identity authentication mechanism firstly;then analyse the advantage and application foregroud of directory service;followly main research four model of LDAP protocol,and deeply study directory information tree;on the foundation of grasping the file format and actualization pricple of LDIF,at first time I implement an automatic generating system of LDIF;and during designing and research, I do some works on designing and optimizing the directory tree ;finally thinking about the actual application in campus network and the good speciality of supporting C/S structure and supporting the different network of LDAP;research and implement the students'information system with uniform identity authentication based on LDAP.

This system mainly includes three aspects of the work:the first is setting up

LDAP server and storing users' account information;the second is designing the application server and connecting with LDAP server;the last is implementing the client;including how to connect with application server and through it connetct with LDAP server;and finishing the data communication between server and client.

Keywords： LDAP,Uniform Identity Authentication,Management System

目　录

第一章　　引言

1.1 研究背景

随着校园网不断的发展，网络的使用由简单的上网，发展到现在的各种应用，网络服务器的种类繁多，用户数量迅速增长，随着校园网络信息的逐渐增加和网络规模的日益扩大，每种应用系统都需要进行身份的识别认证并且对不同身份所拥有的操作权限进行授权。一般的方法是在每一个应用系统中建立独立的身份认证模块，使用独立的认证机制在各自的身份认证文件或数据库中认证。这种管理模式和方法暴露出许多问题，因为每个用户在每个应用系统中都需要建立帐户，所以网络信息的查询及网络管理都变得很不方便，用户办理上网手续往往需要设置多个用户名和口令，如代理账户、拨号账户、Email 账户等，难于记忆和使用，而且用户的管理也不方便，往往会造成数据的不一致性。这样使得我们迫切需要一个统一的、完善的、安全的、易于管理的、有良好的可移植性和扩展性的校园网用户身份管理系统。

目前我国大中小学校网络基础设施建设已初具规模，并为园区用户提供了快速稳定、结构合理的网络通信平台。随之二来的是网络应用的升级。信息技术的不断成熟和网络应用需求的刺激。使得基于校园网络平台的校园信息化建设在今后的网络建设中占有重要的地位，“数字化校园”、“校园一卡通”正在成为网络建设的热点。“数字化校园”建设不可能一蹦而就，需要整体设计、层次化构建、分步实施。集目录服务、身份认证、单点登录技术为一体的基础信息平台建设是数字化校园网的基石，是校园各应用系统协同工作和资源共享的桥梁和纽带。

目录服务[1]为网络中的所有资源提供信息目录，形成一个资源库，集中统一管理所有资源。轻型目录访问协议 LDAP 是基于 TCP/IP 的一个开放的工业标准，它定义了访问和修改目录信息、的标准方法，统一了各种不同的目录，是解决跨平台、跨环境的复杂网络资源管理的重要手段。目前 LDAP 已经得到了广泛的支持和应用，越来越多的生产厂商在自己的产品中增加了支持 LDAP 的这项功能，同时，基于 LDAP 目录服务的应用也越来越广泛，如邮件管理，用户身份，认证管理，公钥管理等等。将 LDAP 目录服务引入到校园网络管理中具有重大的意义，

它的独特优势为校园网提供了一个完整的信息模型和灵活的管理工具。

可以预见，在今后相当长的一段时间里，基于 LDAP 的校园网络管理系统将成为国内外许多学校采用的主要模式之一。

1.2 独立认证的弊端

在校园网信息安全系统建设中，我们首先面对的一个问题就是用户的管理问题，随着校园网的逐步发展，各种基于互联网的应用不断的被开发出来并应用于学校的教学和管理中。今后还会不断增加新的应用系统，用户数量也会不断增加，这样就带来了信息安全方面的两个问题，一是上网的信息资源越多，受黑客攻击的可能性越大(尤其是一些敏感数据)，二是众多用户面对多个应用系统，而各个应用系统都有自己的一套安全策略和用户授权的认证方法，因此，用户不得不记忆不同应用系统的帐号和口令。这种各个应用系统独立认证的方法不论对于用户还是应用系统的开发都是一件麻烦的事情。

独立认证[2]方法的弊端主要有:

✧ 消耗开发成本和延缓应用开发进度。每个应用都要开发一套基本安全系统，是对开发资源的浪费。

✧ 多个认证系统使管理工作成本日益增加，并且越来越不可行。

✧ 用户需要记忆多个帐户和口令，使用极为不便。由于用户口令遗忘而导致的支持费用不断上涨。

✧ 无法统一认证和授权策略。多个认证系统使安全策略必须逐个在不同的系统内进行设置。当应用多达几十个时，修改策略的进度可能跟不上策略的变化。

✧ 无法统一分析用户的应用行为日志格式的不一致.使用户应用行为无法从用户角度进行分析。

1.3 建立 LDAP 统一身份认证的主要优点及发展现状

1.3.1 建立 LDAP 统一身份认证的必要性及主要优点

对于各种网络应用系统，我们可以看做是现实的校园在数字空间的一个映射，即数字校园。在现实校园中，每一个成员都有一个固定的身份，用户的身份决定了用户在校园空间所享有的权限。数字校园是现实校园在数字空间的反映，因此对于数字校园中的每一个成员，在数字空间也相应地需要有一个固定的身份，即电子身份。对于数字校园来说，就是要建立一套统一的身份管理系统，学校的每一个成员都有一个与其身份相应的电子身份，用户可以使用自己的电子身份访问数字校园中有权访问的任何系统。

电子身份的确认需要身份认证技术。身份认证一般与授权控制是相互联系的，授权控制是指一旦用户的身份通过认证以后，确定哪些资源该用户可以访问、可以进行何种方式的访问操作等问题。因此，在数字校园中，应该有一个统一的身份认证系统供各应用系统使用，并且有单一的注册中心统一为各部门服务。

建立了统一的用户身份认证系统[3]，可以方便的实现对用户的统一管理。用户要登录网络，必须先到身份认证系统认证身份，然后才可以访问网络资源，这样，就可以实现基于用户的网络管理。有了用户的认证信息，网络管理人员可以清楚的了解用户使用了那些网络资源，有安全问题发生的时候，可以很快的找到造成问题的用户，从源头上消除安全隐患。

基于 LDAP 的统一身份认证(Uniform Identity Authentication)系统，利用分布式的目录信息树结构，对用户身份信息和系统控制信息进行有效组织和管理，可以提供高效安全的目录访问。在应用系统中都需要进行身份的认证识别并且对不同身份者所拥有的操作权限进行授权。统一身份认证系统的优越性:

- 对身份认证数据规定统一的格式，便于扩充和修改。
- 采用统一的身份信息数据库，避免了各个应用系统的身份信息数据库的数据同步更新问题，同时增加了数据安全性。
- 采用统一的身份认证机制和接口，避免了各种应用系统的重复开发。
- 便于在不同的应用系统之间建立联系，符合应用的实际情况。

1.3.2 国内外 LDAP 身份认证的发展现状

由于身份认证的重要性，所以近年来在技术上得到了飞速的发展。从一般常用的静态口令，动态口令，双因数身份认证，到近来在研究和开发上比较热的PKI数字证书和生物特征技术。但从国外的应用情况及我国的国情来看，与其他几种技术相比较而言，基于口令的身份认证技术使用相对比较广泛，原因在于口令认证使用方便、管理简单、成本低廉。而对于那些要涉及机密数据或者敏感数据的系统，就往往需要采用更高强度的认证技术。

从服务器端认证方式来看，或者说从各个应用系统之间如何交互身份信息角度看，可以把身份认证分为独立认证和统一认证。现在许多应用系统具有一套独立的身份认证子系统，即独立认证，但从安全性、通用性、及时性和权威性来看，都不能令人满意，而且存在很大的安全隐患。

近年也出现了一些统一身份认证的系统，其中一部分是基于LDAP。

◆ 单点登录[4]的问题

在传统模式下，用户登录到每一个应用系统，都要输入一遍帐号和口令信息，然后交由统一身份认证系统来进行身份认证，既显得麻烦，也存在一些安全隐患:

首先，帐号和口令在网络中重复传输，使得口令泄露的风险增加。尽管可以采用一些加密算法来避免口令在网上的直接明文传输，但仍不能保证不会被攻破。在统一认证模式下，这种风险是可怕的，一旦泄露，黑客分子就可以冒充该用户登录所有的应用系统。

其次，用户和应用系统直接连接，假如应用系统是不可信的，或是该应用系统没有足够的安全措施来保护用户的口令等信息，那么也有可能导致口令被不法分子窃取。

因此，统一认证系统还应实现单点登录(single sing-on, SSO)功能。所谓“单点登录”,简单地说，就是通过用户的一次性鉴别登录，即可获得需访问系统和应用软件的授权，在此情况下，管理员无需修改或干涉用户登录就能方便地

实现安全控制。

SSO的机制是“单点登录、全网漫游”，用户访问系统作一次身份认证，随后就可以对所有被授权的网络资源进行无缝访问，而不需要多次输入认证信息。SSO登录，减少了在不同系统中登录所耗费的时间;避免了处理和保存多套系统用户的认证信息;增加了管理的便利性，可以通过直接禁止和删除用户来取消该用户对所有系统资源的访问权限:大大提高了系统的安全性

◆ 对新的应用系统的集成能力

当一个新的应用系统被建立起来后，它希望利用现有的统一身份认证系统对所属用户群进行身份鉴别和授权。在现有模式下，它可能需要和这个认证系统的管理方进行协商，建议管理人员对目录数据库作出相应的改变以集成该应用系统。但这样做往往费时费力。

一个比较好的做法是，统一身份认证系统提供一个应用系统集成的接口，新的应用系统只要提供特定用户群的信息和用户授权策略，认证系统就能对目录数据库做出相应的改动以支持新的应用系统。

◆ 系统间的祸合度问题

由于现有的大多数认证系统采用C/S结构的认证模式，这样带来的一个问题是，一旦服务端的系统结构发生了变化，客户端必须重新调整自己的系统以适应这种变化。如果调用该服务的应用系统数量比较多的话，那么服务端的改变所带来的代价是巨大的和不可接受的。

因此，应尽可能地降低统一身份认证系统和其他应用系统间的祸合度，实现松散藕合，保证服务端的修改不会影响到其他应用系统对该服务的调用。

目前，为解决上述问题，微软和自由联盟(Liberty Alliance)正在致力于基于Web方式的统一身份认证服务的研究，如微软的NET Passport和Sun的Identity Server。 .NET Passport是微软倡导的.NET框架的核心组件之一，是一组联机验证服务的集合。其目的是让用户使用网络和在线购物等电子商务活动更简单和快速。NET Passport是一套基于web的服务，它们的设计目标是简化对安全数据的访问和传输。它把用户的个人注册信息全部存储在微软的服务器上。所有的Passport验证都是通过微软自己的服务器来完成161当用户使用电子邮件地址和密码登陆到允许Passport的，Jeb站点和服务后，如果还需要访问其他支持

passport的站点，就无需再次登陆就可以使用，因此用户无需记住每个网站的不同的登录名和密码。这就实现了所谓的单点登录(single sign-On, SSO)。

1) 自由联盟是用户认证技术的标准化团体，致力于身份鉴定技术。Sun与其他微软的对手已经开始与微软的Passport展开竞争，为用户提供一个在Internet上的数字身份。Liberty反映出两个或多个企业形成一个信任的关系。这种信任可通过企业安排或者合同来缔结。

Liberty信任关系意味着一个企业信任另一个企业的用户认证和身份鉴别。这种信任关系使得用户在一个网站注册后，可以访问另一个网站。因此，Liberty的关键目的在于促进针对于多个站点或者Web服务单一登录。

2).NET Passport和Liberty标准主要是为在因特网大环境中进行的商务活动和个人的网上冲浪而设计的，如B2C 13213，对于数字化校园这种特定的小环境还不适用。一方面，数字化校园的很多应用系统不是面向大众的，比如人事工资系统，档案管理系统.所以这些专用系统是不能加入到Liberty或者Passport中;另一方面，这类统一身份认证系统只是适合基于Web应用的统一认证，而数字化校园中有很多应用系统是非Web方式的应用，如果使用现有的统一认证服务来进行集成，其移植成本和整合难度必然很高。

3）现成的国内外高校 LDAP 应用系统[5]

在 X. 5 00 的基础上，经过了 LDAPvl， LDAPv2， LDAPv3 三个阶段的发展，LD.AP 已经相当成熟。国内外有许多高校都在校园网管理系统中使用了 LDAP 目录服务，国外的如 Stanford University， University of British Columbia,

国内的如清华人学、北京大学,深圳大学等。研究的方向主要有:继续研究 LDAP 协议本身的缺点，如使用专有的 LDIF 格式进行数据交换，使互操作性受到影响;实现网络设备 LDAP 客户端应用程序，完成基于目录的设备配置自动管理;

网络 QoS 的策略管理和目录服务结合;网络管理中 SNMP 和 LDAP 的结合;采用元目录技术等。

1.4 论文研究的主要内容与所做的主要工作